JOURNAL OF NUMBER THEORY **63**, 1–11 (1997)
ARTICLE NO. NT972084

Norm and Trace of the *j*-invariants of Drinfeld Modules Associated to Hyperelliptic Curves

Zesen Chen and David R. Hayes*

University of Massachusetts at Amherst, Amherst, Massachusetts

Communicated by D. Goss

Received May 10, 1996; revised July 10, 1996

Let $k/\mathbb{F}_q(x)$ be a quadratic extension that is ramified over the unique pole of x, and let $\mathbf{A}$ be the integral closure of $\mathbb{F}_q[x]$ in k. Then k is the function field analogue

the full ring of integers of an imaginary quadratic number field. In this paper, we compute the degrees of the trace and norm down to $\mathbb{F}_q[x]$ of $j(\phi)$, the j-invariant of ϕ. Our results generalize previous ones where k was assumed to have genus $g = 1$. © 1997 Academic Press

INTRODUCTION

Let $k/\mathbb{F}_q(x)$ be a quadratic extension which is ramified over the unique pole of x, which we denote by ∞ and refer to as the "infinite place" of $\mathbb{F}_q(x)$. Such extensions are analogues in function fields of imaginary quadratic number fields. Using the Riemann–Roch Theorem, we can find polynomials $a(x)$ and $f(x)$ in $\mathbb{F}_q[x]$ such that k is generated over $\mathbb{F}_q(x)$ by a function y satisfying the quadratic equation

$$y^2 + a(x)\, y = f(x). \tag{1}$$

We may further specify that $f(x)$ is monic of odd degree $n = 2g + 1$ and that $\deg a(x) \leqslant g$, where g is the genus of k. We may choose $f(x)$ and $a(x)$ so that the affine model of k defined by (1) is smooth. If q is odd, we take $a(x) = 0$, and then the smoothness of the affine model (1) is equivalent to $f(x)$ being square free. Since (1) is smooth, the affine coordinate ring $\mathbf{A} = \mathbb{F}_q[x, y]$ is integrally closed in k.

Let ∞ also denote the unique extension of ∞ to k, and let k_∞ be the completion of k at ∞. Let v_∞ be the normalized valuation on k_∞, and for

* Supported in part by NSF Grant DMS-8903512.

0022-314X/97 $25.00

$t \in k_\infty$ define $\deg^*(t) = -v_\infty(t)$. Because of the ramification, we have $\deg^*(t) = 2\deg(t)$ for all $t \in \mathbb{F}_q(x)$. For an integral ideal $\mathfrak{a}$ of $\mathbf{A}$, we define $\deg^* \mathfrak{a} = \dim_{\mathbb{F}_q}(\mathbf{A}/\mathfrak{a})$. When $\mathfrak{a} = \mathbf{A}w$ is principal, $\deg^* \mathfrak{a} = \deg^* w$ because then $\mathfrak{a}$ is the divisor of zeros of w. One knows that $\deg^*$ is a multiplicative function on ideals. It therefore extends uniquely to a multiplicative function on the group of fractional ideals of $\mathbf{A}$.

The element $\pi_\infty = x^g/y$ is a uniformizer in k_∞, and therefore determines a unique sign function $\operatorname{sgn}: k_\infty \to \mathbb{F}_q$ such that $\operatorname{sgn}(\pi_\infty) = 1$. Since x^n/y^2 is a 1-unit at ∞, $\operatorname{sgn}(x) = \operatorname{sgn}((x^n/y^2)\,\pi_\infty^{-2}) = 1$, and $\operatorname{sgn}(y) = \operatorname{sgn}(x^g/\pi_\infty) = 1$ also.

Let ϕ be a rank-one Drinfeld $\mathbf{A}$-module of generic characteristic. Then ϕ is the analogue over k of an elliptic curve with complex multiplications by the full integer ring of an imaginary quadratic number field. In this paper, we compute the degrees of the trace and norm down to $\mathbb{F}_q[x]$ of the j-invariant $j(\phi)$ of ϕ. As $j(\phi)$ is an isomorphism invariant, we can assume that ϕ is sgn-normalized. (See Section 12 of [H3] for the theory of sgn-normalization.) Then ϕ is determined by its values

$$\phi_x = x + a\mathbf{F} + \mathbf{F}^2$$
$$\phi_y = y + c_1\mathbf{F} + c_2\mathbf{F}^2 + \cdots + c_n\mathbf{F}^n$$

where $c_n = \operatorname{sgn}(y) = 1$ and $a, c_1, \ldots, c_{n-1} \in H$, the Hilbert class field of $\mathbf{A}$. The Frobenius endomorphism $\mathbf{F}$ satisfies $\mathbf{F}c = c^q\mathbf{F}$ for any c in the algebraic closure of k. For this ϕ, $j(\phi) = a^{q+1}$.

In [D-H], the degrees of the polynomials $J(\phi) = \operatorname{Norm}_{H \to \mathbb{F}_q(x)}(j(\phi))$ and $\operatorname{Tr}(\phi) = \operatorname{Trace}_{H \to \mathbb{F}_q(x)}(j(\phi))$ are computed when $g = 1$. Equation (1) then defines an elliptic curve over $\mathbb{F}_q$. One finds that $\deg Tr(\phi) = (q+1)\,q^2$ and $\deg J(\phi) = (q+1)(q^2 + q(h-1))$, where h is the class number of k. We will generalize these results to arbitrary genus g.

The Artin map $\mathfrak{a} \mapsto \sigma_\mathfrak{a}$ induces a natural isomorphism from the ideal class group $\operatorname{Pic}(\mathbf{A})$ onto the Galois group $G = \operatorname{Gal}(H/k)$. Let $\mathfrak{a}_1 = \mathbf{A}$ and $\mathfrak{a}_i$, $i = 2, 3, \ldots, h$, be a set of integral representatives for the ideal class group such that each $\mathfrak{a}_i$ has minimum degree d_i in its class. Our main theorem may then be stated as follows.

THEOREM 1. *We have*

$$\deg^*(a^{\sigma_{\mathfrak{a}_i}}) = q^{g+1-d_i} \tag{2}$$

$$\deg J(\phi) = (q+1) \sum_{i=1}^{h} q^{g+1-d_i} \tag{3}$$

and

$$\deg Tr(\phi) = (q+1)\,q^{g+1}. \tag{4}$$

Equations (3) and (4) follow easily from (2). In order to compute $\deg^*(a^{\sigma_{\mathfrak{a}_i}})$, we will use distinct representations for a according as $\mathbf{A}x$ is or is not prime to $\mathfrak{a}_i$. These representations are introduced in Sections 1.1 and 1.2 below.

What might be an analogue of Theorem 1 for j-invariants of elliptic curves defined over $\mathbb{C}$ and admitting complex multiplications by a maximal order? This question is considered in Section 6 below.

1.1. *Representation of a in Terms of x-Division Points*

Let Λ_x be the $\mathbb{F}_q$-vector space of x-division points for the $\mathbf{A}$-module ϕ. One knows that Λ_x is a cyclic $\mathbf{A}$-module. Since $\phi_x(t) = xt + at^q + t^{q^2}$, we have $\Lambda_x = \{\alpha : \phi_x(\alpha) = 0\}$. Let λ be a generator of Λ_x and put $Y = -\lambda^{q-1}$. Then $x - aY + Y^{q+1} = 0$, and so

$$a = xY^{-1} + Y^q. \tag{5}$$

When $\mathfrak{a}$ is prime to $\mathbf{A}x$, the Artin automorphism $\sigma_{\mathfrak{a}}$ extends to the field $H(\lambda)$ generated by the x-division points of ϕ. By Theorems 4.12 and 5.1 and Equation (5.5) of [H2], if $\mathfrak{a}_i$ is prime to $\mathfrak{m} = \mathbf{A}x$, then

$$\lambda^{\sigma_{\mathfrak{a}_i}} = \xi(x\mathfrak{a}_i^{-1}) \cdot e_{x\mathfrak{a}_i^{-1}}(1)$$

where

$$e_{x\mathfrak{a}_i^{-1}}(t) = t \cdot \prod_{\gamma} \left(1 - \frac{t}{\gamma}\right) \qquad (\gamma \in x\mathfrak{a}_i^{-1} - \{0\})$$

for $t \in k_\infty$ is the Drinfeld exponential. Knowing the Weierstrass gaps of $\mathfrak{a}_i$ and that $\mathfrak{a}_i$ is prime to $\mathbf{A}x$, we may use (6.6) of [H2] to compute

$$\deg^*(\lambda^{\sigma_{\mathfrak{a}_i}}) = \frac{d}{dT} Z_{x\mathfrak{a}_i^{-1}}(T, 1)\Big|_{T=1} \tag{6}$$

where the partial zeta-function $Z_{x\mathfrak{a}_i^{-1}}(T, t)$ is defined in Section 4 below.

In Section 5, we will use (6) to compute $\deg^* a^{\sigma_{\mathfrak{a}_i}}$ when $\mathfrak{a}_i$ is prime to $\mathbf{A}x$.

1.2. *Representation of a When* $\mathbf{A}x$ *Splits or Ramifies in* $k/\mathbb{F}_q(x)$

The representation (5) is always valid. However, if $\mathbf{A}x$ splits or ramifies in $k/\mathbb{F}_q(x)$, then we can derive a second representation for a. Let $\mathbf{A}x = \mathfrak{p}\mathfrak{q}$. By Section 4 of [H3], we may decompose ϕ_x as follows in $H[\mathbf{F}]$:

$$\begin{aligned}\phi_x &= (\mathfrak{q} * \phi)_{\mathfrak{p}}\, \phi_{\mathfrak{q}} = [D(\mathfrak{q} * \phi)_{\mathfrak{p}} + \mathbf{F}] \cdot [D(\phi_{\mathfrak{q}}) + \mathbf{F}] \\ &= [D(\phi_{\mathfrak{p}})^{\sigma_{\mathfrak{q}}} + \mathbf{F}] \cdot [D(\phi_{\mathfrak{q}}) + \mathbf{F}] = x + a\mathbf{F} + \mathbf{F}^2.\end{aligned}$$

Therefore

$$x = D(\phi_{\mathfrak{p}})^{\sigma_{\mathfrak{q}}} D(\phi_{\mathfrak{q}}) \qquad \text{and} \qquad a = D(\phi_{\mathfrak{p}})^{\sigma_{\mathfrak{q}}} + D(\phi_{\mathfrak{q}})^{q}$$

and so

$$a = xY^{-1} + Y^{q} \tag{7}$$

once more but now with $Y = D(\phi_{\mathfrak{q}})$. From [H1], we have

$$D(\phi_{\mathfrak{q}}) = \frac{\xi(\mathfrak{q}^{-1})}{\xi(\mathbf{A})} \qquad \text{and} \qquad D(\phi_{\mathfrak{q}})^{\sigma_{\mathfrak{a}}} = \frac{\xi(\mathfrak{q}^{-1}\mathfrak{a}^{-1})}{\xi(\mathfrak{a}^{-1})}. \tag{8}$$

Further, it is shown in [H2] that for any fractional ideal $\mathfrak{a}$,

$$\deg^{*} \xi(\mathfrak{a}) = \frac{d}{dT} V_{\mathfrak{a}}(T)\bigg|_{T=1}, \tag{9}$$

where the partial zeta function $V_{\mathfrak{a}}(T)$ is defined in Section 4 below.

In Section 5, we will use (9) to compute $\deg^{*} a^{\sigma_{\mathfrak{a}_i}}$ when $\mathfrak{a}_i$ and $\mathbf{A}x$ have a common prime factor.

2. HERMITE NORMAL FORM FOR INTEGRAL IDEALS

Since any nonzero ideal $\mathfrak{b} \subseteq \mathbf{A}$ is a rank two $\mathbb{F}_q[x]$-submodule of $\mathbf{A}$, we know from the Hermite normal form that there are uniquely determined polynomials C, D, F in $\mathbb{F}_q[x]$ with C, D both monic and $\deg E < \deg C$ such that

$$\mathfrak{b} = \mathbb{F}_q[x] \cdot C + \mathbb{F}_q[x] \cdot (Dy - E). \tag{10}$$

However, $\mathfrak{b}$ has additional structure. From $y\mathfrak{b} \subset \mathfrak{b}$, we deduce the existence of polynomials A, B such that $yC = BC + A(Dy - E)$. It follows from this equation that $C = AD$ and $E = BD$. We conclude that $\mathfrak{b} = D \cdot \mathfrak{a}$ where

$$\mathfrak{a} = \mathbb{F}_q[x] \cdot A + \mathbb{F}_q[x] \cdot (y - B) \tag{11}$$

with B monic and $\deg B < \deg A$. We observe from (11) that $\mathfrak{a} \cap \mathbb{F}_q[x]$ is generated by A. The inclusion of $\mathbb{F}_q[x]$ in $\mathbf{A}$ therefore induces a monomorphism $\mathbb{F}_q[x]/(A) \to \mathbf{A}/\mathfrak{a}$, and this monomorphism is surjective since $y \equiv B \pmod{\mathfrak{a}}$. It follows that

$$\deg^{*} \mathfrak{a} = \deg A \tag{12}$$

and therefore that

$$\begin{aligned}\deg^* \mathfrak{b} &= \deg^* D + \deg^* \mathfrak{a} = 2 \deg D + \deg A \\ &= \deg(D^2 A) = \deg(CD). \end{aligned} \tag{13}$$

We write $N(\mathfrak{b}) = CD = AD^2$, and we call $N(\mathfrak{b})$ the *polynomial norm* of $\mathfrak{b}$.

DEFINITION 1. An ideal $\mathfrak{a} \subseteq \mathbf{A}$ is *pure* if the only ideal of $\mathbb{F}_q[x]$ dividing $\mathfrak{a}$ is the unit ideal.

Pure ideals clearly have an $\mathbb{F}_q[x]$-basis of type (11). The ideals $\mathfrak{a}_i$ are pure because each is minimal in its class. Therefore, for each $1 \leqslant i \leqslant h$, there exists a monic polynomial A_i and a polynomial B_i with $\deg B_i < \deg A_i$ such that

$$\mathfrak{a}_i = \mathbb{F}_q[x] \cdot A_i + \mathbb{F}_q[x] \cdot (y - B_i). \tag{14}$$

Further, we have $\deg A_i = \deg^* \mathfrak{a}_i = d_i \leqslant g$. This results from the following proposition, which is an analogue of the Minkowski bound.

PROPOSITION 1. *For each class* $\mathfrak{C}$ *in the Picard group* $\mathrm{Pic}(\mathbf{A})$ *of the coordinate ring* $\mathbf{A}$, *there exists an integral ideal* $\mathfrak{a}$ *with* $\deg^* \mathfrak{a} \leqslant g$.

Proof. Pick an integral ideal $\mathfrak{b} \in \mathfrak{C}^{-1}$. By the Riemann–Roch Theorem (see Section 3 below), there exists $z \in \mathfrak{b}$ such that $\deg^* z \leqslant g + \deg^* \mathfrak{b}$. For the integral ideal $\mathfrak{a}$ such that $\mathbf{A}z = \mathfrak{a}\mathfrak{b}$, we have $\deg^* \mathfrak{a} = \deg^* z - \deg^* \mathfrak{b} = g$. Finally, $\mathfrak{a} \in (\mathfrak{C}^{-1})^{-1} = \mathfrak{C}$. ∎

3. GAPS FOR IDEALS IN A

Let $\mathfrak{a}$ be a fixed fractional ideal of $\mathbf{A}$. For integers $v \geqslant 0$, we define $F_v = F_v(\mathfrak{a}) = \{a \in \mathfrak{a} : \deg^* a = v + \deg^* \mathfrak{a}\}$.

DEFINITION 2. If $\mu \geqslant 0$ and $F_\mu(\mathfrak{a})$ is empty, then μ is called a gap number for $\mathfrak{a}$ or simply a *gap*. Otherwise, μ is called a *non-gap number* for $\mathfrak{a}$.

For any divisor D of k, let $L(D)$ be the set of all $y \in k$ such that $v_w(yD) \geqslant 0$ at every place w of k, and put $\ell(D) = \dim_{\mathbb{F}_q} L(D)$. For $r \geqslant 0$, we define $T_r = T_r(\mathfrak{a}) = L(\mathfrak{a}^{-1} \infty^{r + \deg^* \mathfrak{a}}) = \{0\} \cup (\bigcup_{v=0}^{r} F_v)$. The Riemann–Roch Theorem implies that $\dim_{\mathbb{F}_q}(T_{r+1}/T_r)$ is zero or one and that $\dim_{\mathbb{F}_q}(T_r) = r + 1 - g$ for $r \geqslant 2g - 1$. Thus T_{2g-1} has dimension g, and so there are exactly g gaps and g non-gaps for $0 \leqslant v \leqslant 2g - 1$.

LEMMA 1. *Let* $\mu_0 < \mu_1 < \cdots < \mu_{g-1}$ *be the non-gaps for* $\mathfrak{a}$. *Then*

$$|F_{\mu_s}| = q^s(q-1).$$

Proof. Immediate from the fact that $\dim_{\mathbb{F}_q}(T_{r+1}/T_r)$ is zero or one. ∎

LEMMA 2. *For a pure integral ideal* $\mathfrak{a}$ *such that* $\deg^* \mathfrak{a} = d \leqslant g$, *the non-gaps are the integers* $\mu = d + 2s$ *for* $s = 0, ..., g-d-1$ *and* $\mu = 2g - d + s$ *for* $s = 0, ..., d-1$.

Proof. In the Hermite Normal Form (11) for $\mathfrak{a}$, we have $\deg^* A = 2d \leqslant 2g$ and $\deg^*(y - B) = 2g + 1$. Thus, there are no elements $a \in \mathfrak{a}$ with $\deg^* a < 2d$ and also no elements a with $\deg^* a$ odd and less than $2g+1$. Thus, $v = t$ for $0 \leqslant t < d$ and $v = d + 1 + 2t$ for $0 \leqslant t < g - d$ are g gaps for $\mathfrak{a}$. The remaining $\mu < 2g$ are therefore the non-gaps. ∎

COROLLARY 1. *The pure ideals* $\mathfrak{a}$ *with* $\deg^* \mathfrak{a} \leqslant g$ *are exactly the minimal ideals* $\mathfrak{a}_i$, $1 \leqslant i \leqslant h$, *representing the class group* $\mathrm{Pic}(\mathbf{A})$.

Proof. The gaps and non-gaps of an ideal $\mathfrak{a}$ are invariants of its ideal class because $\alpha \mapsto z\alpha$ is an isomorphism of $T_r(\mathfrak{a})$ onto $T_r(z\mathfrak{a})$. The above lemma shows that the first non-gap of any pure ideal $\mathfrak{a}$ with $d = \deg^* \mathfrak{a} \leqslant g$ is its degree d. Therefore, such an ideal must be minimal in its class. ∎

COROLLARY 2. *For* $1 \leqslant i \leqslant h$, *we have*

$$|F_\mu(\mathfrak{a}_i)| = q^s(q-1) \tag{15}$$

for $\mu = d_i + 2s$ *with* $0 \leqslant s \leqslant g - d_i - 1$, *and*

$$|F_\mu(\mathfrak{a}_i)| = q^{(g-d_i+s)}(q-1). \tag{16}$$

for $\mu = 2g - d_i + s$ *with* $0 \leqslant s \leqslant d_i - 1$. *Otherwise*, $|F_v(\mathfrak{a}_i)| = 0$.

Proof. Immediate from Lemmas 1 and 2. ∎

DEFINITION 3. Given a fractional ideal $\mathfrak{a}$ of $\mathbf{A}$, let $d(\mathfrak{a})$ denote the minimal degree of an integral ideal in the class of $\mathfrak{a}$.

We note that $d(\mathfrak{a}) = d_i$, where $\mathfrak{a}_i$ is the representative ideal we have chosen in the class of $\mathfrak{a}$.

LEMMA 3. *Let* $\mathfrak{a}$ *be a fractional ideal of* $\mathbf{A}$. *Then, for* $z \neq 0$, $z \in \mathbf{A}$, *each of* $\mathfrak{a}$, $z\mathfrak{a}$ *and* $\mathfrak{a}^{-1}$ *have the same gaps. Further*, $d(\mathfrak{a}) = d(z\mathfrak{a}) = d(\mathfrak{a}^{-1})$.

Proof. We have already observed that the gaps of $\mathfrak{a}$ are invariants of its ideal class. Let $\mathrm{Gal}(k/\mathbb{F}_q(x)) = \{1, c\}$ with $c^2 = 1$. Then $\mathfrak{a}\mathfrak{a}^c = N(\mathfrak{a})$. $\mathbf{A}$ is a principal ideal, so $\mathfrak{a}^{-1}$ and $\mathfrak{a}^c$ are in the same class, and so have the same gaps. Since $\mathfrak{a}$ and $\mathfrak{a}^c$ have the same gaps, $\mathfrak{a}$ and $\mathfrak{a}^{-1}$ also have the same gaps. Finally, $d(\mathfrak{a}^{-1}) = d(\mathfrak{a}^c) = d(\mathfrak{a}) = d(z\mathfrak{a})$. ∎

4. PARTIAL ZETA FUNCTIONS

Let $\mathfrak{a}$ be any fractional ideal of $\mathbf{A}$. The formal power series

$$\zeta_{\mathfrak{a}}(T) = \frac{1}{q-1} \sum_{a \in \mathfrak{a} - \{0\}} T^{\deg^* a - \deg^* \mathfrak{a}} \tag{17}$$

depends only on the ideal class of $\mathfrak{a}$. It is known to define a rational function of T, which we will compute explicitly below. We will employ (17) in evaluating the formal power series

$$V_{\mathfrak{a}}(T) = \sum_{a \in \mathfrak{a} - \{0\}} T^{\deg^* a} = (q-1) \cdot T^{\deg^* \mathfrak{a}} \cdot \zeta_{\mathfrak{a}}(T) \tag{18}$$

and the formal power series

$$Z_{\mathfrak{a}}(T, t) = \sum_{a \in \mathfrak{a}} T^{\deg^*(a+t)},$$

which is defined for all $t \in k - \mathfrak{a}$. Both these series are rational functions of T (see, e.g., Section 6 of [H2]).

LEMMA 4. *If* $\deg^* \mathfrak{a} + d(\mathfrak{a}) > 0$, *then*

$$Z_{\mathfrak{a}}(T, 1) = 1 + (q-1) \cdot T^{\deg^* \mathfrak{a}} \cdot \zeta_{\mathfrak{a}}(T)$$

as formal power series.

Proof. By Lemmas 2 and 3, the first non-empty layer $F_v(\mathfrak{a})$ of $\mathfrak{a}$ occurs at $v = d(\mathfrak{a})$. Thus, all elements of $\mathfrak{a}$ have degree no less than $\deg^* \mathfrak{a} + d(\mathfrak{a}) > 0$. So $1 \notin \mathfrak{a}$, and further $\deg^*(a+1) = \deg^*(a)$ for all $a \in \mathfrak{a} - \{0\}$. ∎

PROPOSITION 2. *Setting* $d = d(\mathfrak{a})$, *we have*

$$\zeta_{\mathfrak{a}}(T) = \frac{T^d}{1 - qT^2} - \frac{q^{g+1-d} T^{2g+1-d} (T-1)}{(1-qT)(1-qT^2)} \tag{19}$$

for any fractional ideal $\mathfrak{a}$.

Proof. From the definitions and Corollary 2,

$$(q-1)\cdot\zeta_{\mathfrak{a}}(T)=\sum_{\mu=0}^{\infty}|F_{\mu}(\mathfrak{a})|\,T^{\mu}$$
$$=\sum_{s=0}^{g-d-1}q^{s}(q-1)\,T^{d+2s}+\sum_{s=0}^{\infty}q^{g-d+s}(q-1)\,T^{2g-d+s}$$
$$=(q-1)\left(T^{d}\sum_{s=0}^{g-d-1}(qT^{2})^{s}+q^{g-d}T^{2g-d}\sum_{s=0}^{\infty}(qT)^{s}\right).$$

We conclude that

$$\zeta_{\mathfrak{a}}(T)=T^{d}\frac{1-q^{g-d}T^{2g-2d}}{1-qT^{2}}+\frac{q^{g-d}T^{2g-d}}{1-qT}$$
$$=\frac{T^{d}}{1-qT^{2}}+q^{g-d}T^{2g-d}\left(\frac{1}{1-qT}-\frac{1}{1-qT^{2}}\right)$$

as required.

COROLLARY 3. *We have* $\zeta_{\mathfrak{a}}(1)=1/(1-q)$ *and*

$$\left.\frac{d}{dT}\zeta_{\mathfrak{a}}(T)\right|_{T=1}=\frac{2-d}{q-1}+\frac{2-q^{g+1-d}}{(q-1)^{2}}. \tag{20}$$

COROLLARY 4. *We have*

$$\left.\frac{d}{dT}V_{\mathfrak{a}}(T)\right|_{T=1}=-\deg^{*}\mathfrak{a}+2-d+\frac{2-q^{g+1-d}}{q-1}. \tag{21}$$

Proof. This follows easily from (18) and Corollary 3. ∎

COROLLARY 5. *Put* $d=d(\mathfrak{a})$. *If* $\deg^{*}\mathfrak{a}+d>0$, *then*

$$\left.\frac{d}{dT}Z_{\mathfrak{a}}(T,1)\right|_{T=1}=-\deg^{*}\mathfrak{a}+2-d+\frac{2-q^{g+1-d}}{q-1}. \tag{22}$$

Proof. This follows easily from Lemma 4 and Corollary 3. ∎

5. PROOF OF THE MAIN THEOREM

To complete the proof of Theorem 1, we must evaluate the derivatives on the right hand sides of (6) and (9). Assume first that $\mathfrak{a}_i$ is prime to $\mathbf{A}x$.

The condition of Corollary 5 holds for $\mathfrak{a} = x\mathfrak{a}_i^{-1}$ because $d(x\mathfrak{a}_i^{-1}) = d(\mathfrak{a}_i) = d_i$ by Lemma 3. Therefore (22) implies that

$$\begin{aligned}\deg^*(\lambda^{\sigma_{\mathfrak{a}_i}}) &= \frac{d}{dT} Z_{x\mathfrak{a}_i^{-1}}(T, 1)\Big|_{T=1} \\ &= -\deg^*(x\mathfrak{a}_i^{-1}) + 2 - d_i + \frac{2 - q^{g+1-d_i}}{q-1} \\ &= \frac{2 - q^{g+1-d_i}}{q-1}\end{aligned}$$

as $\deg^*(x) = 2$. Thus

$$\deg^*(Y^{\sigma_{\mathfrak{a}_i}}) = (q-1) \cdot \deg^*(\lambda^{\sigma_{\mathfrak{a}_i}}) = 2 - q^{g+1-d_i}. \tag{23}$$

This evaluation is valid for all the $\mathfrak{a}_i$ that are prime to $\mathbf{A}x$. If $\mathfrak{a}_i$ is not prime to $\mathbf{A}x$, then $\mathbf{A}x = \mathfrak{p}\mathfrak{q}$ is a product of first degree primes. We may assume that $\mathfrak{a}_i = \mathfrak{p}\mathfrak{b}$. Then, with $Y = D(\phi_{\mathfrak{q}})$, we have from (8)

$$Y^{\sigma_{\mathfrak{a}_i}} = \frac{\xi(\mathfrak{q}^{-1}\mathfrak{a}_i^{-1})}{\xi(\mathfrak{a}_i^{-1})} = \frac{\xi(\mathfrak{q}^{-1}\mathfrak{p}^{-1}\mathfrak{b}^{-1})}{\xi(\mathfrak{a}_i^{-1})} = \frac{\xi(x^{-1}\mathfrak{b}^{-1})}{\xi(\mathfrak{a}_i^{-1})} = x \cdot \frac{\xi(\mathfrak{b}^{-1})}{\xi(\mathfrak{a}_i^{-1})}$$

so that

$$\begin{aligned}\deg^*(Y^{\sigma_{\mathfrak{a}_i}}) &= \deg^*(x) + \deg^* \xi(\mathfrak{b}^{-1}) - \deg^* \xi(\mathfrak{a}_i^{-1}) \\ &= 2 + \frac{d}{dT} V_{\mathfrak{b}^{-1}}(T)\Big|_{T=1} - \frac{d}{dT} V_{\mathfrak{a}_i^{-1}}(T)\Big|_{T=1} \\ &= 2 + \frac{(2 - q^{g+1-(d_i-1)}) - (2 - q^{g+1-d_i})}{q-1} \\ &= 2 - q^{g+1-d_i}\end{aligned}$$

by Corollary 4 as $\deg^*(\mathfrak{a}_i^{-1}) = -d_i$ and $d(\mathfrak{b}^{-1}) = \deg^*(\mathfrak{b}) = d_i - 1$.

We are now in a position to prove (2). Put $Y_i = Y^{\sigma_{\mathfrak{a}_i}}$. Then by either (5) or (7), as the case may be, we have

$$a^{\sigma_{\mathfrak{a}_i}} = xY_i^{-1} + Y_i^q$$

with $\deg^*(Y_i) = 2 - q^{g+1-d_i}$. Since $\deg^*(xY_i^{-1}) = 2 - \deg^*(Y_i) = q^{g+1-d_i} > 0$ while $\deg^*(Y_i^q) = q(2 - q^{g+1-d_i}) \leqslant 0$, we find

$$\deg^*(a^{\sigma_{\mathfrak{a}_i}}) = \deg^*(xY_i^{-1}) = q^{g+1-d_i},$$

which is the statement (2). Both (3) and (4) follow easily from (2).

6. ELLIPTIC CURVES WITH COMPLEX MULTIPLICATION

Let $k = \mathbb{Q}(\sqrt{D})$ be an imaginary quadratic number field of discriminant $D < 0$, and let $\mathcal{O}_k$ be the ring of integers of k. Under an embedding $\mathbf{e}: k \to \mathbb{C}$, each fractional ideal $\mathfrak{a}$ of $\mathcal{O}_k$ maps to a rank two lattice $\mathbf{e}(\mathfrak{a})$ in $\mathbb{C}$. The j-invariant $j(\mathfrak{a})$ of the lattice is then the j-invariant of the elliptic curve $E(\mathfrak{a}) \cong \mathbb{C}/\mathfrak{a}$ with complex multiplications by $\mathcal{O}_k$. Let h_k be the class number of k, and choose a set of representatives $\mathfrak{a}_1 = \mathcal{O}_k$ and $\mathfrak{a}_i$ for $2 \leqslant i \leqslant h_k$ for the ideal class group $\mathrm{Pic}(\mathcal{O}_k)$. As is well known, $H_k = k(j(\mathfrak{a}))$ is the Hilbert class field of k and both

$$\mathrm{Tr}(E(\mathcal{O}_k)) := \mathrm{Trace}_{H \to \mathbb{Q}}\, j(E(\mathcal{O}_k))$$

and

$$J(E(\mathcal{O}_k)) := \mathrm{Norm}_{H \to \mathbb{Q}}\, j(E(\mathcal{O}_k)) = \left| \prod_{i=1}^{h_k} j(\mathfrak{a}_i) \right|^2$$

are integers. In [G-Z], Gross and Zagier find bounds for the valuations $v_p(J(E(\mathcal{O}_k))$ at rational primes p. One can also ask for bounds on the "valuations" $-\log |\mathrm{Tr}(E(\mathcal{O}_k))|$ and $-\log |J(E((\mathcal{O}_k))|$ at the archimedean place of $\mathbb{Q}$. In particular, we can try to state an analogue for Theorem 1 with $\log |\mathrm{Tr}(E(\mathcal{O}_k))|$ and $\log |J(E(\mathcal{O}_k))|$ viewed as analogues for $\deg Tr(\phi)$ and $\deg J(\phi)$.

If $\omega = (D + \sqrt{D})/2$, then $\mathcal{O}_k = \mathbb{Z} + \mathbb{Z}\omega$. By the Hermite Normal Form (cf. [C]), for any fractional ideal $\mathfrak{a}$, there is a rational number $d > 0$ and integers $a > 0$ and b such that $\mathfrak{a} = d \cdot (\mathbb{Z}a + \mathbb{Z}(\omega - b))$. Choosing $\sqrt{D}$ so that $\mathbf{e}(\sqrt{D})$ sits in the upper half-plane, we may compute

$$j(\mathfrak{a}) = j\left(\frac{\omega - b}{a}\right)$$

where

$$j(\tau) = \frac{1}{q} + 744 + \cdots$$

is the modular function. Since

$$|q| = |e^{2\pi i(\omega - b)/a}| = e^{-\pi \sqrt{|D|}/a},$$

the Fourier series for $j(\tau)$ will converge fastest if we choose a as small as possible. Therefore, for $1 \leqslant i \leqslant h_k$, choose $\mathfrak{a}_i$ to be the integral ideal of

minimal norm in its class, and let a_i be the norm of $\mathfrak{a}_i$. If we approximate the modular function by the first term of its Fourier series, then we have

$$\log |j(\mathfrak{a}_i)| \sim \log |e^{\pi \sqrt{|D|}/a_i}| = \pi \sqrt{|D|}/a_i \tag{24}$$

and

$$\log J(E(\mathcal{O}_k)) = \sum_{i=1}^{h_k} 2 \log |j(\mathfrak{a}_i)| \sim 2\pi \sum_{i=1}^{h_k} \sqrt{|D|}/a_i. \tag{25}$$

In the function field setting, the analogue of $\sqrt{|D|}$ is

$$\sqrt{q^{\deg f(x)}} = \sqrt{q^{2g+1}} = \sqrt{q}\, q^g.$$

Therefore, (24) is an analogue of (2) if we take $\sqrt{q}$ as an analogue of π!

The approximation (24) is very good when $a_i << \sqrt{|D|}$. For example, when $D = -163$, we have $h_k = 1$, $j(E(\mathcal{O}_k)) = -262537412640768000$, and $J(E(\mathcal{O}_k)) = j(E(\mathcal{O}_k))^2$; and we find

$$\left| \frac{\log J(E(\mathcal{O}_k))}{2\pi \sqrt{163}} - 1 \right| \leqslant 7.07 \times 10^{-7}.$$

It is known (see [C]) that $a_i < \sqrt{|D|/3}$. However, computation reveals many examples when a_i approaches this bound. In that case, some integer translate of $(\omega - b)/a_i$ may be very near to the cusp $(\pm 1 + \sqrt{-3})/2$ of the fundamental domain for $j(\tau)$, and the approximation will be poor.

REFERENCES

[C] H. Cohen, "A Course in Computational Number Theory," Springer-Verlag, New York/Berlin/Heidelberg, 1993.

[D-H] D. S. Dummit and D. R. Hayes, Rank-one Drinfeld modules on elliptic curves, *Math. Comput.* **62** (1994), 875–883.

[G-Z] B. Gross and D. Zagier, On singular moduli, *J. Reine Angew. Math.* **355** (1985), 191–220.

[H1] D. R. Hayes, Elliptic units in function fields, *in* "Number Theory Related to Fermat's Last Theorem," Proceedings of the Conference Sponsored by the Vaughn Foundation, pp. 321–340, Birkhäuser, Boston, 1982.

[H2] D. R. Hayes, Stickelberger elements in function fields, *Compositio Math.* **55** (1985), 209–239.

[H3] D. R. Hayes, A brief introduction to Drinfeld modules, *in* "The Arithmetic of Function Fields, Proceedings of the Workshop at Ohio State University, June 17–26, 1991," pp. 1–32, De Gruyter, Berlin/New York, 1992.